IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) [[An]] A cryptographic processing apparatus for performing Feistel-type common-key-block cryptographic processing, ~~having~~ comprising:

a ~~structure~~ processor that repeatedly executes an SPN-type F-function having a nonlinear conversion section and a linear conversion section over a plurality of rounds, wherein

each of the linear conversion ~~section~~ sections of an F-function corresponding to each of the plurality of rounds is configured to perform linear conversion processing of an input of n [[bit]] bits outputted from each of [[the]] m nonlinear conversion sections, ~~totally~~ in total mn [[bit]] bits, as linear conversion processing that applies a square MDS (Maximum Distance Separable) matrix, at least in [[the]] consecutive odd-numbered rounds and in [[the]] consecutive even-numbered rounds, different square MDS matrices L_a, L_b are applied, and

a matrix composed of m ~~column~~ row vectors selected arbitrarily from ~~column~~ row vectors constituting inverse matrices L_a^{-1}, L_b^{-1} of the square MDS matrices is linearly independent.

2. (Currently Amended) The cryptographic processing apparatus for performing the Feistel-type common-key-block cryptographic processing according to claim 1, wherein

a matrix composed of m ~~column~~ row vectors selected arbitrarily from ~~column~~ row vectors constituting the inverse matrices L_a^{-1}, L_b^{-1} is a square MDS matrix.

3. (Original) The cryptographic processing apparatus for performing the Feistel-type common-key-block cryptographic processing according to claim 1, wherein

an algorithm of the Feistel-type common-key-block cryptographic processing is a cryptographic algorithm of round number 2r, and

the linear conversion section of the F-function is configured to execute linear conversion applying q kinds of different square MDS matrices ($2 \leq q < r$) sequentially and repeatedly in all of the r even-numbered rounds and in all of the r odd-numbered rounds.

4. (Currently Amended) The cryptographic processing apparatus for performing the Feistel-type common-key-block cryptographic processing according to claim 1, wherein

each of the plurality of different square MDS matrices to be applied in the linear conversion section of the F-function is a square MDS matrix that is composed of m ~~column~~ row vectors selected arbitrarily from ~~column~~ row vectors constituting the plurality of square MDS matrices and is linearly independent.

5. (Currently Amended) The cryptographic processing apparatus for performing the Feistel-type common-key-block cryptographic processing according to claim 1, wherein

each of the plurality of different square MDS matrices to be applied in the linear conversion section of the F-function is a square MDS matrix such that a matrix composed of m ~~column~~ row vectors selected arbitrarily from ~~column~~ row vectors constituting the plurality of square MDS matrices is also a square MDS matrix.

6. (Cancelled)

7. (Currently Amended) An cryptographic processing method implemented by a cryptographic processing device configured to perform ~~for performing~~ Feistel-type common-key-block cryptographic processing, the method comprising ~~the steps of~~:

executing, by the cryptographic processing device, an SPN-type F-function for performing nonlinear conversion processing and linear conversion processing repeatedly over a plurality of rounds; and

in the conversion processing of an F-function corresponding to each of the plurality of rounds, performing linear conversion for n [[bit]] bits outputted from the m nonlinear conversion sections, ~~totally~~ in total mn [[bit]] bits, as linear conversion processing applying square MDS (Maximum Distance Separable) matrices[;], wherein

linear conversion processing with square MDS matrices such that at least in [[the]] consecutive even-numbered rounds and in [[the]] consecutive odd-numbered rounds different square MDS matrices L_a, L_b are applied, and a matrix composed of m ~~column~~ row vectors selected arbitrarily from ~~column~~ row vectors constituting the inverse matrices L_a^{-1}, L_b^{-1} of the square MDS matrices is linearly independent and makes up a square MDS matrix.

8. (Currently Amended) The cryptographic processing method for performing the Feistel-type common-key-block cryptographic processing according to claim 7, wherein

linear conversion processing by square MDS matrices such that a matrix composed of m ~~column~~ row vectors selected arbitrarily from ~~column~~ row vectors constituting the inverse matrices L_a^{-1}, L_b^{-1} is a square MDS matrix.

9. (Original) The cryptographic processing method for performing the Feistel-type common-key-block cryptographic processing according to claim 7, wherein

an algorithm of the Feistel-type common-key-block cryptographic processing is a cryptographic algorithm of round number 2r, and the linear conversion processing of the F-function executes linear conversion processing sequentially and repeatedly applying q kinds of different square MDS matrices ($2 \leq q < r$).

10. (Currently Amended) The cryptographic processing method for performing the Feistel-type common-key-block cryptographic processing according to claim 7, wherein

each of the plurality of different square MDS matrices to be applied to the linear conversion processing of the F-function is such that a matrix composed of m ~~column~~ row vectors selected arbitrarily from ~~column~~ row vectors constituting the plurality of square MDS matrices is linearly dependent and makes up a square MDS matrix.

11. (Currently Amended) The cryptographic processing method for performing the Feistel-type common-key-block cryptographic processing according to claim 7, wherein

each of the plurality of different square MDS matrices to be applied to linear conversion processing of the F-function is a square MDS matrix such that a matrix composed of m ~~column~~ row vectors selected arbitrarily from the ~~column~~ row vectors constituting the plurality of square MDS matrices becomes a square MDS matrix.

12. (Cancelled)

13. (Currently Amended) A computer readable medium storing a program, which when executed by a computer, causes the computer to perform ~~program of performing the~~ Feistel-type common-key-block cryptographic processing ~~according to claim 7~~, comprising the [[step]] steps of:

executing an SPN-type F-function for performing nonlinear conversion processing and linear conversion processing over a plurality of rounds, wherein

the linear conversion processing of the F-function corresponding to each of the plurality of rounds is a linear conversion step of performing linear conversion processing for n [[bit]] bits outputted from the m nonlinear conversion sections, ~~totally~~ in total mn [[bit]] bits, as linear conversion processing applying a square MDS (Maximum Distance Separable) matrix, and

in the linear conversion step, linear conversion processing by square MDS matrices is executed in such a way that at least in [[the]] consecutive even-numbered rounds and in [[the]] consecutive odd-numbered rounds, different square MDS matrices are applied, and a matrix composed of m ~~column~~ row vectors selected arbitrarily from ~~column~~ row vectors constituting inverse matrices L_a^{-1}, L_b^{-1} of the square MDS matrices is linearly independent.

14. (New) An encryption processing apparatus, comprising:

a first encryption processing section, including

a first nonlinear transformation unit configured to transform from input information to first nonlinear transformed information; and

a first linear transformation unit configured to transform from said nonlinear transformed information to first linear transformed information;

a second encryption processing section, including

a second nonlinear transformation unit configured to transform from input information to second nonlinear transformed information; and

a second linear transformation unit configured to transform from said nonlinear transformed information to second linear transformed information; and an exclusive-or section configured to perform an exclusive-or operation based on said second linear transformed information and said first linear transformed information,

wherein when said first nonlinear transformed information is expressed as a first sequence vector, said first linear transformed information is expressed as a second sequence vector, said second nonlinear transformed information is expressed as a third sequence vector, and said second linear transformed information is expressed as a fourth sequence vector, a first row vector chosen from an inverse matrix of a first matrix, which indicates transformation from said first sequence vector to said second sequence vector, and a second row vector chosen from an inverse matrix of said second matrix, which indicates a transformation from said third sequence vector to said fourth sequence vector, are linearly independent.

15. (New) The encryption apparatus according to claim 14, further comprising:

a key acquiring section configured to acquire the common key which is used in a decryption apparatus.

16. (New) The encryption apparatus according to claim 14, further comprising:

a key expanded section configured to output expanded keys, and wherein one of the expanded keys is inputted to the first encryption processing section, and the other of the expanded keys is inputted to the second encryption processing section.

17. (New) An encryption processing apparatus comprising:

a first encryption processing means, including

a first nonlinear transformation means for transforming from input information to first nonlinear transformed information; and a first linear transformation means for transforming from said nonlinear transformed information to first linear transformed information;

a second encryption processing means, including

a second nonlinear transformation means for transforming from input information to second nonlinear transformed information; and

a second linear transformation means for transforming from said nonlinear transformed information to second linear transformed information; and

an exclusive-or means for performing an exclusive-or operation based on said second linear transformed information and said first linear transformed information,

wherein when said first nonlinear transformed information is expressed as a first sequence vector, said first linear transformed information is expressed as a second sequence vector, said second nonlinear transformed information is expressed as a third sequence vector, and said second linear transformed information is expressed as a fourth sequence vector, a first row vector chosen from an inverse matrix of a first matrix, which indicates transformation from said first sequence vector to said second sequence vector, and a second row vector chosen from an inverse matrix of said second matrix, which indicates a transformation from said third sequence vector to said fourth sequence vector, are linearly independent.

18. (New) An encryption method, comprising:

a first encryption step including transforming from input information to first nonlinear transformed information, and transforming from said nonlinear transformed information to first linear transformed information;

a second encryption step including transforming from input information to second nonlinear transformed information, and transforming from said nonlinear transformed information to second linear transformed information; and

performing an exclusive-or operation based on said second linear transformed information and said first linear transformed information,

wherein when said first nonlinear transformed information is expressed as a first sequence vector, vector, said first linear transformed information is expressed as a second sequence vector, and said second nonlinear transformed information is expressed as a third sequence vector, a first row vector chosen from an inverse matrix of a first matrix, which indicates transformation from said first sequence vector to said second sequence vector, and a second row vector chosen from an inverse matrix of said second matrix, which indicates a transformation from said third sequence vector to said fourth sequence vector, are linearly independent.

19. (New) The encryption method according to claim 18, further comprising:

acquiring the common key which is used in a decryption apparatus.

20. (New) The encryption method according to claim 18, further comprising:

outputting expanded keys.

21. (New) A decryption processing apparatus, comprising:

a first decryption processing section, including

a first nonlinear transformation unit configured to transform from input information to first nonlinear transformed information; and a first linear transformation unit configured to transform from said nonlinear transformed information to first linear transformed information;

a second decryption processing section, including

a second nonlinear transformation unit configured to transform from input information to second nonlinear transformed information; and

a second linear transformation unit configured to transform from said nonlinear transformed information to second linear transformed information; and

an exclusive-or section configured to perform an exclusive-or operation based on said second linear transformed information and said first linear transformed information,

wherein when said first nonlinear transformed information is expressed as a first sequence vector, said first linear transformed information is expressed as a second sequence vector, said second nonlinear transformed information is expressed as a third sequence vector, and said second linear transformed information is expressed as a fourth sequence vector, a first row vector chosen from an inverse matrix of a first matrix, which indicates transformation from said first sequence vector to said second sequence vector, and a second row vector chosen from an inverse matrix of said second matrix, which indicates a transformation from said third sequence vector to said fourth sequence vector, are linearly independent.

22. (New) The decryption processing apparatus according to claim 21, further comprising:

a key acquiring section configured to acquire the common key which is used in an encryption apparatus.

23. (New) The decryption processing apparatus according to claim 21, further comprising:

a key expanded section configured to output expanded keys, and wherein one of the expanded keys is inputted to the first decryption processing section, and the other of the expanded keys is inputted to the second decryption processing section.

24. (New) A decryption processing apparatus, comprising:

a first decryption processing means including

a first nonlinear transformation means for transforming from input information to first nonlinear transformed information; and

a first linear transformation means for transforming from said nonlinear transformed information to first linear transformed information;

a second decryption processing means including

a second nonlinear transformation means for transforming from input information to second nonlinear transformed information; and

a second linear transformation means for transforming from said nonlinear transformed information to second linear transformed information; and

an exclusive-or means for performing an exclusive-or operation based on said second linear transformed information and said first linear transformed information, wherein

when said first nonlinear transformed information is expressed as a first sequence vector, said first linear transformed information is expressed as a second sequence vector, said second nonlinear transformed information is expressed as a third sequence vector, and said second linear transformed information is expressed as a fourth sequence vector, a first row vector chosen from an inverse matrix of a first matrix, which indicates transformation from said first sequence vector to said second sequence vector, and a second row vector chosen from an inverse matrix of said second matrix, which indicates a transformation from said third sequence vector to said fourth sequence vector, are linearly independent.

25. (New) A decryption method, comprising:

a first decryption step including transforming from input information to first nonlinear transformed information, and transforming from said nonlinear transformed information to first linear transformed information;

a second decryption step including transforming from input information to second nonlinear transformed information, and transforming from said nonlinear transformed information to second linear transformed information; and

performing an exclusive-or operation based on said second linear transformed information and said first linear transformed information,

wherein when said first nonlinear transformed information is expressed as a first sequence vector, said first linear transformed information is expressed as a second sequence vector, said second nonlinear transformed information is expressed as a third sequence vector, and said second linear transformed information is expressed as a fourth sequence vector, a first row vector chosen from an inverse matrix of a first matrix, which indicates transformation from said first sequence vector to said second sequence vector, and a second row vector chosen from an inverse matrix of said second matrix, which indicates a transformation from said third sequence vector to said fourth sequence vector, are linearly independent.

26. (New) The decryption method according to claim 25, further comprising:

acquiring the common key which is used in decryption apparatus.

27. (New) The decryption method according to claim 25, further comprising:

outputting expanded keys.